IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): A. Juels
Case: 4414-35
Serial No.: 10/782,309
Filing Date: February 19, 2004
Group: 2635
Examiner: William L. Bangachon

Title: Low-Complexity Cryptographic Techniques for use with Radio Frequency Identification Devices

---

TRANSMITTAL OF APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith are the following documents relating to the above-identified patent application:

(1) Appeal Brief; and
(2) Copy of Notice of Appeal, filed on November 2, 2005, with copy of stamped return postcard indicating receipt of Notice by PTO on November 7, 2005.

There is an additional fee of $500 due in conjunction with this submission under 37 CFR §1.17(c). Please charge **Ryan, Mason & Lewis, LLP Account No. 50-0762** the amount of $500, to cover this fee. In the event of non-payment or improper payment of a required fee, the Commissioner is authorized to charge or to credit **Deposit Account No. 50-0762** as required to correct the error. A duplicate copy of this letter is enclosed.

Respectfully submitted,

Joseph B. Ryan

Date: January 9, 2006

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517

Attorney Docket No. 4414-35

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): A. Juels
Case: 4414-35
Serial No.: 10/782,309
Filing Date: February 19, 2004
Group: 2635
Examiner: William L. Bangachon

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature Lisa M. Hasli Date: January 9, 2006

Title: Low-Complexity Cryptographic Techniques for use with Radio Frequency Identification Devices

---

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant hereby appeals the final rejection dated August 2, 2005 of claims 1-16, 20 and 23-33 of the above-identified application.

REAL PARTY IN INTEREST

The present application is currently assigned to RSA Security Inc. RSA Security Inc. is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no known related appeals or interferences.

STATUS OF CLAIMS

The present application was filed on February 19, 2004, with claims 1-33. The present application claims priority to U.S. provisional application Serial No. 60/468,200, filed May 6,

2003. Claims 1-33 remain pending in the present application. Claims 1 and 30-33 are the independent claims.

Claims 1-16, 20 and 23-33 stand rejected under 35 U.S.C. §103(a). Claims 17-19, 21 and 22 are indicated as containing allowable subject matter. Claims 1-16, 20 and 23-33 are appealed.

STATUS OF AMENDMENTS

There have been no amendments filed subsequent to the final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 is directed to a method for use in an RFID system. The RFID system comprises at least one RFID device and at least one reader which communicates with the RFID device. An example of an RFID system can be seen in FIG. 1 of the drawings, which shows an RFID system 100 comprising RFID tags 102 which communicate with a reader 104. See the specification at page 6, lines 1-6. The method includes the steps of associating a plurality of pseudonyms with the RFID device, and transmitting from the RFID device different ones of the pseudonyms in response to different reader queries of the RFID device. An authorized verifier, which may be the reader or another system entity, is able to determine that the different transmitted pseudonyms are associated with the same RFID device. An example of an authentication protocol carried out between the verifier and one of the tags 102 of system 100 is shown in FIG. 3 of the drawings, and is described in the specification at page 12, line 17, to page 14, line 14.

Independent claims 30, 31 and 32 are respective device, reader and system versions of method claim 1. Examples of the claimed device, reader and system may be seen in the respective RFID tag 102, reader 104 and system 100 of FIG. 1.

Independent claim 33 is directed to a method for use in a system comprising at least one device and at least one reader which communicates with the device. The method includes the steps of associating a plurality of pseudonyms with the device, and transmitting from the device different ones of the pseudonyms in response to different reader queries of the device. The claim further recites that the pseudonyms are determined utilizing an updateable set of one or more one-time pads maintained in the device. An example of a system in which the method is implemented is system 100 of FIG. 1, comprising RFID tags 102 and reader 104. An illustrative

embodiment utilizing an updatable set of one or more one-time pads is described in greater detail in the specification at page 9, line 12, to page 10, line 25.

The claimed arrangements advantageously overcome significant problems of the prior art. For example, as noted at page 2, lines 12-25, conventional cryptographic techniques for authenticating tags are often "far too complex to implement within the limited computational and storage capabilities typical of existing RFID tags." By transmitting different pseudonyms from a given RFID device in response to different reader queries of the given device, the stated problem is overcome in a manner which "involves no computationally-intensive cryptographic operations, and relatively little storage, making it practical for implementation in low-cost RFID tags and other devices." See the specification at, for example, page 4, lines 11-15, and page 7, line 24, to page 8, line 21.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1, 2, 4-8, 20, 23-25, 30, 32 and 33 are rejected under 35 U.S.C. §103(a) over U.S. Patent No. 6,842,106 (hereinafter "Hughes") in view of U.S. Patent No. 4,928,098 (hereinafter "Dannhaeuser").

2. Claims 3 and 31 are rejected under 35 U.S.C. §103(a) as being unpatentable over Hughes and Dannhaeuser in view of U.S. Patent No. 6,724,895 (hereinafter "Turner").

3. Claims 9-16 and 26-29 are rejected under 35 U.S.C. §103(a) as being unpatentable over Hughes and Dannhaeuser in view of U.S. Patent No. 6,225,889 (hereinafter "Furuta").

ARGUMENT

1. §103(a) Rejection of Claims 1, 2, 4-8, 20, 23-25, 30, 32 and 33

Claims 1, 2, 4, 23-25, 30 and 32

A proper *prima facie* case of obviousness requires that the combination of references must teach or suggest all the claim limitations, and that there be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine or modify the reference teachings. See Manual of Patent Examining Procedure (MPEP), Eighth Edition, August 2001, §706.02(j).

Applicant submits that the Examiner has failed to establish a proper *prima facie* case of obviousness in the §103(a) rejection of independent claim 1, in that the collective disclosures of

Hughes and Dannhaeuser fail to teach or suggest all the claim limitations, and in that no cogent motivation has been identified for combining or modifying the reference teachings to reach the claimed invention.

As noted above, independent claim 1 is directed to a method for use in an RFID system comprising at least one RFID device and at least one reader which communicates with the RFID device. The method includes the steps of associating a plurality of pseudonyms with the RFID device, and transmitting from the RFID device different ones of the pseudonyms in response to different reader queries of the RFID device. The claim further specifies that an authorized verifier is able to determine that the different transmitted pseudonyms are associated with the same RFID device.

Applicant notes that an RFID device, by its very nature, necessarily transmits device-identifying information. See the specification at, for example, page 1, line 19, to page 2, line 15, and page 4, line 28, to page 5, line 26.

It is also important to note that claim 1 requires the association of a plurality of pseudonyms with an RFID device, with different ones of the pseudonyms being transmitted by the device in response to different reader queries of the RFID device. A given reader query of an RFID device constitutes a request for the device-identifying information of that device, as is apparent from, for example, page 5, lines 24-26, of the specification.

In the invention of claim 1, an authorized verifier, which may be a reader, is able to determine that the different transmitted pseudonyms are associated with the same RFID device. This advantageously results in an arrangement in which the RFID device can be authenticated without the need for complex cryptographic operations, thereby overcoming a significant problem of the prior art. See the specification at, for example, page 2, lines 12-25, and page 4, lines 11-15.

The Examiner argues that the proposed combination of Hughes and Dannhaeuser teaches each and every limitation of claim 1. Applicant respectfully disagrees. In formulating the rejection, the Examiner argues that the secret key value 66 stored in memory 50 of each tag 44 in Hughes constitutes one or more pseudonyms as claimed. See the final Office Action at page 6, last paragraph. However, the secret key value 66 cannot reasonably be construed as comprising a plurality of pseudonyms, or even a single pseudonym. As noted above, a pseudonym as that term is used in the present specification and in standard usage implies some ability to identify a

particular entity with which the pseudonym is associated. In the Hughes system, the same secret key value 66 is stored in each of the tags 44, as indicated at column 5, lines 47-50. Thus, the secret key value itself does not provide any device-identifying information whatsoever, and accordingly is not a pseudonym for the device. Instead, Hughes teaches to use a conventional identification code to identify a particular tag to the reader. See Hughes at, for example, column 5, lines 7-8 and 21-23. The tags in the Hughes system are therefore configured to "broadcast their identifiers in a promiscuous manner to any nearby readers." See the specification at page 2, lines 12-15. Hughes addresses this problem through the use of a complex challenge-response authentication process, of the type referred to at page 2, lines 16-22, of the specification, rather than through the use of pseudonyms as claimed. Thus, Hughes is believed to teach away from the claimed arrangements.

In addition, the Hughes approach suffers from exactly the same problem identified by Applicant at page 2, lines 12-22, of the specification, in that it requires an unduly complex cryptographic arrangement in order to provide authentication. As indicated previously, the claimed arrangements advantageously overcome this problem.

Moreover, Applicant notes that the secret key value 66 is apparently not transmitted by any of the RFID tags in Hughes. As noted above, claim 1 calls for the transmission of different pseudonyms of an RFID device in response to different reader queries of that device. The Examiner argues that the secret key value 66 meets the claimed pseudonym, but such a value is not transmitted by its corresponding device, as would be required by explicit recitations in claim 1. The pseudorandom values that are processed using the secret key value 66 and transmitted as part of the Hughes challenge-response authentication process do not constitute pseudonyms as claimed, again because such pseudorandom values do not provide any device-identifying information. Thus, Hughes appears to teach directly away from the present invention, and suffers from the same problem that is advantageously addressed and solved by the claimed arrangements.

The Examiner acknowledges that Hughes alone fails to meet the limitations of claim 1, but argues that the deficiencies of Hughes are overcome by Dannhaeuser. However, the automobile remote keyless entry codes in Dannhaeuser do not constitute pseudonyms as claimed, because the codes do not provide any ability to uniquely identify a particular code transmitting device. In the remote keyless entry context of the Dannhaeuser system, it is well known that for

a given automobile, the owner is typically provided with multiple redundant remote keyless entry devices. The codes shown in the table in column 3 of Dannhaeuser would therefore have to be replicated on each such device. As a result, the codes themselves cannot be used to uniquely identify any particular one of the multiple devices. The Dannhaeuser codes are therefore not pseudonyms as recited in the claim. Moreover, because the Dannhaeuser devices do not transmit device-identifying information, those devices are not RFID devices as claimed.

It should be pointed out in this regard that remote keyless entry devices would not be understood by one skilled in the art to constitute RFID devices of the type recited in the claim at issue. Remote keyless entry devices simply transmit a code which if found to match a code in a corresponding receiver causes the receiver to perform some action, such as unlocking a car. See Dannhaeuser at, for example, column 1, lines 14-24, and column 5, line 32, to column 6, line 2. RFID devices, on the other hand, emit device-identifying information in response to a reader query, thereby allowing the reader to uniquely identify the particular device with which it is communicating. Thus, it is believed that RFID devices and remote keyless entry devices are entirely different types of devices, and one looking to improve an RFID device would generally not look to the remote keyless entry device art. The Dannhaeuser teachings are therefore believed to represent non-analogous art relative to the Hughes reference.

Accordingly, it is believed that the collective teachings of Hughes and Dannhaeuser fail to meet the pseudonym transmission aspects of claim 1.

Inasmuch as claim 1 includes limitations not taught or suggested by the combined teachings of Hughes and Dannhaeuser, the Examiner has failed to establish a *prima facie* case of obviousness for this claim.

Also, as indicated previously, the Examiner has failed to identify a cogent motivation for combining the Hughes and Dannhaeuser references or for modifying their teachings to reach the claimed invention. The claimed arrangement advantageously overcomes the above-noted problems associated with the conventional approach of configuring RFID tags to "broadcast their identifiers in a promiscuous manner to any nearby readers." Hughes, by teaching use of such an identifier broadcasting approach in conjunction with challenge-response authentication, directly teaches away from the claimed invention, and fails to provide its associated advantages. Similarly, Dannhaeuser teaches to transmit remote keyless entry codes, which may be replicated on multiple devices and hence do not uniquely identify any particular device. Accordingly, there

is no objective evidence of record which would lead one skilled in the art to combine or modify Hughes and Dannhaeuser to reach the claimed invention.

The Federal Circuit has stated that when patentability turns on the question of obviousness, the obviousness determination "must be based on objective evidence of record" and that "this precedent has been reinforced in myriad decisions, and cannot be dispensed with." In re Sang-Su Lee, 277 F.3d 1338, 1343 (Fed. Cir. 2002). Moreover, the Federal Circuit has stated that "conclusory statements" by an examiner fail to adequately address the factual question of motivation, which is material to patentability and cannot be resolved "on subjective belief and unknown authority." Id. at 1343-1344. As noted above, there has been no showing in the present §103(a) rejection of claim 1 of objective evidence of record that would motivate one skilled in the art to combine or modify the Hughes and Dannhaeuser references to produce the particular limitations in question.

Instead of objective evidence of motivation to combine or modify Hughes and Dannhaeuser, the Examiner simply provides conclusory statements. For example, the Examiner states that it would be obvious to combine Hughes and Dannhaeuser "because it provides security to a wireless communication by foiling attempts of code grabbers from copying and re-using a single transmitted pseudonym to be used in unauthorized accesses." See the final Office Action at page 7, second paragraph.

The Examiner apparently argues that it would be obvious to apply the remote keyless entry code rotation process of Dannhaeuser to the secret key value 66 of Hughes to provide improved security. However, such an arrangement would clearly be undesirable in an RFID system having a very large number of tags. Hughes teaches that the same secret key value 66 is stored in each of the tags. In a typical RFID system, there are thousands of such tags. If the Dannhaeuser code rotation were applied to the secret key value 66 of Hughes, it would appear to be very difficult and highly impractical to coordinate such secret key value rotation between all the tags and the reader. The rotation is possible in the Dannhaeuser automobile remote keyless entry context because there are usually only a few remote keyless entry devices per automobile. Moreover, Hughes provides a challenge-response authentication process to address the security issue raised by the Examiner, and thus there is no apparent need in the Hughes system for code rotation of the type disclosed in Dannhaeuser. Accordingly, it is believed that the Dannhaeuser technique is not only undesirable in an RFID system, it is practically unworkable in such a

system. It is also contrary to the objectives of the claimed invention in terms of providing techniques implementable in low-cost RFID devices with limited computational and storage resources.

It therefore appears that the Examiner in formulating the §103(a) rejection of claim 1 over Hughes and Dannhaeuser has undertaken a piecemeal reconstruction of the claimed invention based upon impermissible hindsight, given the benefit of the disclosure provided by Applicant.

Moreover, it should be noted that the Dannhaeuser teachings were made available to the public in 1990, upon publication of the corresponding patent document. Conventional RFID systems have also been well known for many years. One cannot help but wonder why those skilled in the art, despite long exposure to the teachings of Dannhaeuser as well as conventional RFID systems, have not heretofore made the combination that is alleged to be obvious by the Examiner. This failure of others to develop the advantageous approach set forth in the present application is believed to constitute strong evidence of non-obviousness.

Thus, the §103(a) rejection of claim 1 over Hughes and Dannhaeuser is believed to be improper, and should be withdrawn.

Dependent claims 2, 4 and 23-25 are believed allowable for at least the reasons identified above with regard to independent claim 1.

Independent claims 30 and 32 include limitations similar to those of independent claim 1, and are therefore believed allowable for reasons similar to those identified above.

Claim 5

Dependent claim 5 specifies that the verifier authenticates itself to the RFID device by releasing to the RFID device an authentication value β_i unique to a given pseudonym α_i transmitted by the RFID device. The Examiner argues that this limitation is met by the teachings in column 7, lines 16-23, of Hughes. Applicant respectfully disagrees. The relied-upon portion does not teach or suggest an authentication value unique to a given pseudonym, as recited. Instead, a reader sends an encrypted challenge value to the tag, where the challenge value is a random number previously supplied by the tag to the reader. Accordingly, the collective teachings of Hughes and Dannhaeuser fail to meet the limitation in question.

Claim 6

Dependent claim 6 specifies that the RFID device authenticates itself to the verifier by releasing to the verifier an authentication value γ_i unique to a given pseudonym α_i transmitted by the RFID device. The Examiner argues that this limitation is met by the teachings in column 7, lines 24-31, of Hughes. Applicant respectfully disagrees. The relied-upon portion does not teach or suggest an authentication value unique to a given pseudonym, as recited. Instead, the "challenge response" transmitted by the tag is an encrypted "challenge value" that was previously received by the tag from the reader. Accordingly, the collective teachings of Hughes and Dannhaeuser fail to meet the limitation in question.

Claim 7

Dependent claim 7 specifies that at least one of the pseudonyms comprises an identifier of the RFID device. The Examiner argues that this limitation is met by the tag key values in column 6, lines 57-65, of Hughes. However, these values do not constitute RFID device identifiers. Moreover, key values are not transmitted by an RFID device in Hughes, and hence cannot read on the claimed pseudonyms. Accordingly, the collective teachings of Hughes and Dannhaeuser fail to meet the limitation in question.

Claim 8

Dependent claim 8 specifies that at least one of the pseudonyms comprises a portion of an identifier of the RFID device. The Examiner argues that this limitation is met by the tag key values in column 6, lines 60-62, of Hughes. However, these values do not constitute portions of RFID device identifiers. Moreover, key values are not transmitted by an RFID device in Hughes, and hence cannot read on the claimed pseudonyms. Accordingly, the collective teachings of Hughes and Dannhaeuser fail to meet the limitation in question.

Claim 20

Dependent claim 20 specifies that a verifier of the system is configured to store for a given RFID device T_x a static identifier id_x corresponding to at least one pseudonym of T_x. The Examiner argues that this limitation is met by FIG. 3 of Dannhaeuser. Applicant respectfully disagrees. First, there is no FIG. 3 in Dannhaeuser. Second, there are no RFID device

pseudonyms disclosed in Dannhaeuser. Accordingly, the collective teachings of Hughes and Dannhaeuser fail to meet the limitation in question.

Claim 33

Applicant initially notes with regard to claim 33 that the Examiner is incorrect in stating at page 9, second to last paragraph, of the final Office Action that claim 33 "recites the limitations of claim 1." Claim 33 does not include the wherein clause of claim 1, and does not refer to an RFID system or RFID devices. See the specification at, for example, page 5, lines 2-7. As noted previously herein, claim 33 recites that pseudonyms are determined utilizing an updatable set of one or more one-time pads maintained in a device. The Examiner argues that the claimed updatable set of one or more one-time pads is disclosed by the "index designators" in column 4, lines 5-24, of Dannhaeuser. Applicant respectfully disagrees. As is well known to one skilled in the cryptographic arts, a "one-time pad" is a type of cryptographic construct, an example of which is described in the specification at page 10, lines 11-17. The relied-upon portion of Dannhaeuser makes no reference whatsoever to any aspect of cryptography, much less to one-time pads as claimed.

Applicant notes that the foregoing reference to a cryptographic construct cannot reasonably be viewed as arguing a limitation that is not present in the claim. A one-time pad is in fact a cryptographic construct, as indicated in the specification and as is well known to those skilled in this art, and the relied-upon portions of Dannhaeuser do not provide any disclosure regarding one-time pads. Hughes, like Dannhaeuser, makes no reference to one-time pads. As a result, the obviousness rejection of claim 33 based on Hughes and Dannhaeuser is fundamentally flawed and should be withdrawn.

Applicant brought these deficiencies regarding the stated rejection of claim 33 to the attention of the Examiner in a response filed November 2, 2005, but the Examiner has apparently declined to take any action to correct them. See the November 2, 2005 response at page 7, paragraphs 5 and 6, and the subsequent Advisory Action dated November 28, 2005.

2. §103(a) Rejection of Claims 3 and 31

Claim 3

Dependent claim 3 is believed allowable for at least the reasons identified above with regard to independent claim 1. The Turner reference fails to overcome the fundamental deficiencies of Hughes and Dannhaeuser as identified above.

Claim 31

Independent claim 31 includes limitations similar to those of independent claim 1, and is therefore believed allowable for reasons similar to those identified above. The Turner reference fails to overcome the fundamental deficiencies of Hughes and Dannhaeuser as identified above.

Applicant further notes with regard to claim 31 that the Examiner at page 4, last line, of the final Office Action, states that claim 31 "recites the combination of claims 1 and 3." Also, on page 10, second paragraph, the Examiner characterizes claim 31 as reciting "a system for practicing the combination of method claims 1 and 3." These characterizations of claim 31 are clearly incorrect. For example, claim 3 specifies that "transmitted pseudonyms are authenticated by a verifier other than the reader." This limitation is not present in claim 31. Also, claim 31 recites a plurality of RFID devices and a plurality of readers, while claim 1 recites at least one RFID device and at least one reader. Accordingly, the above-noted characterizations regarding claim 31 are improper and should be withdrawn.

As with claim 33, Applicant brought these deficiencies regarding the stated rejection of claim 31 to the attention of the Examiner in the response filed November 2, 2005, but the Examiner has apparently declined to take any action to correct them. See the November 2, 2005 response at page 2, paragraph 6, and the Advisory Action dated November 28, 2005.

3. §103(a) Rejection of Claims 9-16 and 26-29

Claims 9-16

Dependent claims 9-16 are believed allowable for at least the reasons identified above with regard to independent claim 1. The Furuta reference fails to overcome the fundamental deficiencies of Hughes and Dannhaeuser as identified above.

Claim 26

Dependent claim 26 specifies that the RFID device generates the plurality of pseudonyms as pseudonyms $\alpha_1 = f(1)$, $\alpha_2 = f(2)$, ..., $\alpha_k = f(k)$. The Examiner argues that this limitation is met by the teachings in column 8, lines 60-65, of Furuta. However, the relied-upon portion does not disclose generation of pseudonyms as a sequence of outputs of a pseudorandom number generator, as recited. Accordingly, the collective teachings of Hughes, Dannhaeuser and Furuta fail to meet the limitation in question.

Claim 27

Dependent claim 27 specifies that the RFID device and a verifier of the system attempt to maintain a common counter d_x unique to the RFID device, and share the seed κ_x. The Examiner argues that this limitation is met by the teachings in column 5, lines 46-50, of Hughes. However, Applicant has been unable to locate any suggestion in the relied-upon portion, or elsewhere in Hughes, Dannhaeuser and Furuta, regarding the particular common counter and seed sharing arrangement set forth in the claim. It is believed that the collective teachings of Hughes, Dannhaeuser and Furuta fail to meet the limitation in question.

Claim 28

Dependent claim 28 specifies that in order to determine which RFID device is associated with a given incoming value α, the verifier performs a lookup in a list $\{f_{\kappa_x}(d_x)\}$ of current α values for a plurality of RFID devices. The Examiner argues that this limitation is met by the teachings in column 5, lines 8-10 and 21-23, of Hughes. However, Hughes makes no mention of the particular type of lookup recited in the claim, namely, one in which a list of pseudorandom number generator outputs based on a common counter is utilized. It is believed that the collective teachings of Hughes, Dannhaeuser and Furuta fail to meet the limitation in question.

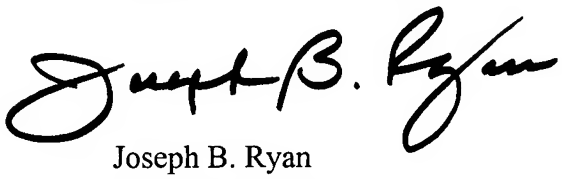
Claim 29

Dependent claim 29 specifies that, for a given counter value d, the RFID device computes $\alpha_d = f(bk + d)$, where b denotes a base value, and the verifier provides a subsequent instruction to the RFID device to increment the base value b. The Examiner argues that this limitation is met by the teachings in column 6, lines 48-52, of Furuta. However, the recited

computation is not disclosed or suggested in the relied-upon portion of Furuta. It is believed that the collective teachings of Hughes, Dannhaeuser and Furuta fail to meet the limitation in question.

In view of the above, Applicant believes that claims 1-16, 20 and 23-33 are in condition for allowance, and respectfully requests the withdrawal of the §103(a) rejections.

Respectfully submitted,



Date: January 9, 2006

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517

CLAIMS APPENDIX

1. A method for use in an RFID system comprising at least one RFID device and at least one reader which communicates with the RFID device, the method comprising the steps of:

associating a plurality of pseudonyms with the RFID device; and

transmitting from the RFID device different ones of the pseudonyms in response to different reader queries of the RFID device;

wherein an authorized verifier is able to determine that the different transmitted pseudonyms are associated with the same RFID device.

2. The method of claim 1 wherein the transmitted pseudonyms are authenticated by the reader.

3. The method of claim 1 wherein the transmitted pseudonyms are authenticated by a verifier other than the reader.

4. The method of claim 1 wherein the RFID device is configured to authenticate itself to a verifier only after the verifier has authenticated itself to the RFID device.

5. The method of claim 4 wherein the verifier authenticates itself to the RFID device by releasing to the RFID device an authentication value β_i unique to a given pseudonym α_i transmitted by the RFID device.

6. The method of claim 4 wherein the RFID device authenticates itself to the verifier by releasing to the verifier an authentication value γ_i unique to a given pseudonym α_i transmitted by the RFID device.

7. The method of claim 1 wherein one or more of the pseudonyms each comprise an identifier of the RFID device.

8. The method of claim 1 wherein one or more of the pseudonyms each comprise a portion of an identifier of the RFID device.

9. The method of claim 1 wherein the pseudonyms are stored in the RFID device as an ordered list of pseudonyms, the method further including the steps of designating a particular one of the pseudonyms as a current pseudonym and, in response to a given reader query, transmitting the current pseudonym, wherein over a plurality of reader queries the pseudonym designated as the current pseudonym periodically cycles through the list of pseudonyms.

10. The method of claim 9 wherein after the current pseudonym is transmitted by the RFID device responsive to the given query, a different one of the plurality of stored pseudonyms is designated as the current pseudonym to be transmitted responsive to a subsequent query.

11. The method of claim 1 wherein one or more of the pseudonyms are generated on an as-needed basis within the RFID device.

12. The method of claim 1 wherein one or more of the pseudonyms are generated externally to the RFID device.

13. The method of claim 1 further including the step of limiting a rate at which the RFID device is permitted to transmit pseudonyms responsive to reader queries.

14. The method of claim 1 further including the step of periodically altering one or more of the plurality of pseudonyms.

15. The method of claim 14 wherein the altering step is implemented responsive to receipt of refresh information in the RFID device from a verifier.

16. The method of claim 15 wherein the refresh information comprises one or more refresh values transmitted from the verifier to the RFID device after mutual authentication of the RFID device and the verifier.

17. The method of claim 1 wherein for a given value κ utilized in the RFID device, a vector $\Delta_\kappa = \{ \delta_\kappa^{(1)}, \delta_\kappa^{(2)}, \ldots, \delta_\kappa^{(m)} \}$ of one-time pads is maintained in the RFID device, wherein the one-time pad $\delta_\kappa^{(1)}$ is designated as a live pad and is used by the RFID device to update the value κ, where m denotes a number of authentication sessions over which one-time pads are constructed.

18. The method of claim 17 wherein the value κ is updated by computing $\kappa \leftarrow \kappa \oplus \delta_\kappa^{(1)}$.

19. The method of claim 17 wherein in conjunction with updating the value κ, the vector Δ_κ is updated utilizing a vector $\widetilde{\Delta}_\kappa = \{\widetilde{\delta}_\kappa^{(1)}, \widetilde{\delta}_\kappa^{(2)}, \ldots, \widetilde{\delta}_\kappa^{(m)}\}$ of one-time pads, the vector Δ_κ being updated by discarding the previous live pad $\widetilde{\delta}_\kappa^{(1)}$, setting $\delta_\kappa^{(i)} = \delta_\kappa^{(i+1)}$ for $1 \leq i \leq n-1$, setting $\delta_\kappa^{(m)} = 0^l$, and performing an element-wise exclusive-or of Δ_κ and $\widetilde{\Delta}_\kappa$ by computing $\delta_\kappa^{(i)} = \delta_\kappa^{(i)} \oplus \widetilde{\delta}_\kappa^{(i)}$, such that the updated vector Δ_κ comprises a set of m one-time pads with decreasing levels of backward secrecy.

20. The method of claim 1 wherein a verifier of the system is configured to store for a given RFID device T_x a static identifier id_x corresponding to at least one pseudonym of T_x.

21. The method of claim 20 wherein the pseudonyms for T_x are obtained by encrypting $id_x \parallel z_x$ under a symmetric key K_α for the verifier, where z_x comprises a pseudonym counter.

22. The method of claim 21 wherein when the verifier receives a pseudonym from the RFID device, the verifier decrypts the pseudonym using K_α to obtain the corresponding static identifier id_x.

23. The method of claim 1 wherein a verifier of the system in conjunction with an authentication session with the RFID device specifies a value identifying a particular pseudonym to be transmitted by the RFID device.

24. The method of claim 1 wherein the RFID device determines which of the plurality of pseudonyms to transmit responsive to a given reader query based at least in part on timing information.

25. The method of claim 1 wherein the RFID device incorporates a pseudorandom number generator, where $f_{\kappa_x}(i)$ represents an output of the pseudorandom number generator for index i, where κ_x is a seed associated with the RFID device.

26. The method of claim 25 wherein the RFID device generates the plurality of pseudonyms as pseudonyms $\alpha_1 = f(1)$, $\alpha_2 = f(2)$, ..., $\alpha_k = f(k)$.

27. The method of claim 25 wherein the RFID device and a verifier of the system attempt to maintain a common counter d_x unique to the RFID device, and share the seed κ_x.

28. The method of claim 27 wherein in order to determine which RFID device is associated with a given incoming value α, the verifier performs a lookup in a list $\{f_{\kappa_x}(d_x)\}$ of current α values for a plurality of RFID devices.

29. The method of claim 27 wherein for a given counter value d, the RFID device computes $\alpha_d = f(bk + d)$, where b denotes a base value, and the verifier provides a subsequent instruction to the RFID device to increment the base value b.

30. An apparatus for use in an RFID system, the apparatus comprising:

an RFID device having a plurality of pseudonyms associated therewith and being operative to communicate with one or more readers of the system;

the RFID device being further operative to transmit different ones of the pseudonyms in response to different reader queries of the RFID device;

wherein an authorized verifier is able to determine that the different transmitted pseudonyms are associated with the same RFID device.

31. An RFID system comprising:

a plurality of RFID devices; and

a plurality of readers which communicate with at least a subset of the RFID devices;

wherein a plurality of pseudonyms are associated with a given one of the RFID devices, the given RFID device being configurable to transmit different ones of the pseudonyms in response to different reader queries of the given RFID device;

wherein an authorized verifier is able to determine that the different transmitted pseudonyms are associated with the same RFID device.

32. An apparatus for use in an RFID system, the apparatus comprising:

a reader which communicates with one or more RFID devices;

wherein a plurality of pseudonyms are associated with a given one of the RFID devices, the given RFID device transmitting different ones of the pseudonyms in response to different reader queries of the given RFID device;

wherein an authorized verifier is able to determine that the different transmitted pseudonyms are associated with the same RFID device.

33. A method for use in a system comprising at least one device and at least one reader which communicates with the device, the method comprising the steps of:

associating a plurality of pseudonyms with the device; and

transmitting from the device different ones of the pseudonyms in response to different reader queries of the device;

wherein the pseudonyms are determined utilizing an updateable set of one or more one-time pads maintained in the device.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None

PTO/SB/31 (04-05)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

NOTICE OF APPEAL FROM THE EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Docket Number (Optional): 4414-35

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]
on November 2, 2005
Signature: V. Bencivenni
Typed or printed name: V. Bencivenni

In re Application of: Ari Juels

Application Number	Filed
10/782,309	February 19, 2004

For: Low-Complexity Cryptographic Techniques for Use with Radio Frequency Identification Devices

Art Unit	Examiner
2635	William L. Bangachon

Applicant hereby **appeals** to the Board of Patent Appeals and Interferences from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 41.20(b)(1)) $ 500.00

- ☐ Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by half, and the resulting fee is: $ _____
- ☐ A check in the amount of the fee is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The Director has already been authorized to charge fees in this application to a Deposit Account. I have enclosed a duplicate copy of this sheet.
- ☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 50-0762 . I have enclosed a duplicate copy of this sheet.
- ☐ A petition for an extension of time under 37 CFR 1.136(a) (PTO/SB/22) is enclosed.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☑ attorney or agent of record. Registration number 37,922
- ☐ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34. _____

Signature: Joseph B. Ryan
Typed or printed name: Joseph B. Ryan
Telephone number: 516-759-7517
Date: November 2, 2005

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

Receipt in the USPTO is hereby acknowledged of:

Transmittal Letter - 1 page
Response to Final Office Action - 8 pages
Notice of Appeal - (Orig. & 1 copy)

November 2, 2005
Serial No. 10/782,309
4414-35